Federal Bureau of Investigation
Office of Public Affairs
National Press Office

Public Affairs Guidance

POC : AD Michael P. Kortan [redacted]
POC: UC [redacted]
PAS [redacted]

b6
b7C

Topic: Going Dark and Encryption

Press Guidance:

Talking Points and Q & A's below are ~~**for internal use only.**~~ Use these to assist preparing SAC or others for any interviews or inquiries. Do not disseminate this paper in this format. Field Offices media reps should handle all local media queries. Calls referring to cases of a national significance can be referred to NPO UC [redacted] or PAS [redacted]

b6
b7C

Background:

[redacted]

b5
b7E

Q & As:

Has the Going Dark problem gotten worse for law enforcement over the past year? How?

The impediments faced by law enforcement have been getting worse for quite some time. The Communications Assistance for Law Enforcement Act (CALEA) was enacted in 1994 and applies only to traditional telecommunications carriers, providers of interconnected Voice over Internet Protocol (VoIP) services, and providers of broadband access services. Today, thousands of companies provide some form of communication service, and most are not required by statute to develop lawful intercept capabilities for law enforcement. As a result,

many of today's communication services are developed and deployed without consideration of law enforcement's lawful intercept and evidence collection needs.

What is the FBI's reaction to the announcement from Apple that their phones will include encryption that the company is not able to unlock, even in response to a court order? How will this impact the FBI's investigative abilities?

The FBI continues to be extremely concerned about the serious threat posed by the increasing proliferation of encryption technology that prevents timely access to critical evidence obtained through legal process. Law enforcement needs the cooperation and assistance from industry in complying with lawful court orders so that criminals around the world cannot seek safe haven for lawless conduct.

What about workarounds? Can't law enforcement retrieve the same information through metadata, the Cloud, or through guessing the password on the phone?

While law enforcement may be able to obtain some information from communications service providers such as telephone records, email logs, and location information, that information is difficult to access when time is of the essence, and does not provide the content of any communication.

The FBI may be able to access data stored in the Cloud with a search warrant. But backing a device up to the Cloud does not include all of the stored data on a particular device (e.g., phone, laptop, tablet). The missing information can create a black hole for law enforcement. If a device is not routinely backed up to the Cloud, or if a target opts out of backing up to the Cloud, some of the data can only be found on the encrypted device.

As for guessing the password, many devices have a setting whereby data is erased after too many failed attempts to access a locked device.

Many adversaries pay close attention to law enforcement's diminishing set of capabilities and continually seek ways to exploit the gaps. It is vital that capabilities to access the types of information needed to protect the public safety and national security of our country are maintained.

Has the FBI experienced any reduced cooperation from communication providers as a result of the disclosures attributed to Edward Snowden?

Yes. A number of the country's largest providers have been openly vocal about their concerns regarding surveillance and have published an open letter to the President and members of Congress. Law enforcement has no issue with these companies' commitment to *"keeping users' data secure — deploying the latest encryption technology to prevent unauthorized surveillance on our networks and by pushing back on government requests to ensure that they are legal and reasonable in scope."*

What is missing is a vigorous commitment to assist law enforcement when electronic surveillance of a specific criminal target is authorized pursuant to court order.

What is needed is an open and frank dialogue about the responsibilities of industry to assist law enforcement. Industry and law enforcement need to move forward and develop a framework under which both sides participate in striking an appropriate balance among the public's privacy interests, the industry's goals of competition and innovation, and the ability of law enforcement to protect the public safety.

Why does law enforcement believe companies should be forced to build in

backdoors when designing services? Don't backdoors pose a security risk for companies?

There is a misconception that building a lawful intercept solution into a system requires a so-called "back door," one that foreign adversaries and hackers may try to exploit. Law enforcement is not seeking nor advocating for a back door. Law enforcement wants to use the front door, with clarity and transparency, and with clear guidance provided by law. Front doors can provide the evidence and information needed to investigate crime and prevent terrorist attacks.

Cyber adversaries will exploit any vulnerability they find. It makes more sense to address security risks by developing intercept solutions during the design/development phase, rather than resorting to a patchwork solution when law enforcement serves a court order after the fact. Such solutions are likely to be better, smarter, cheaper, and more secure than solutions that are retrofitted to existing products.

It's important to stress that an open, transparent process for identifying technical capabilities benefits everyone. First, the public can be assured law enforcement is not asking for new authorities. Rather, law enforcement is advocating that industry be able to comply with court orders issued pursuant to existing legal authorities. Second, the industry understands its responsibilities and all providers are held to the same standard (i.e., a level playing field). Third, law enforcement can be confident that it will receive what it needs and is authorized by law to collect, regardless of the specific service provider.

How many companies or applications does the FBI encounter where you know they will not provide real time data?

There are hundreds of communication service providers that offer new services that do not have a lawful intercept capability. This number continues to grow as technology continues to evolve. Some providers of new services may have a partial capability to provide data periodically. However, the capabilities are incomplete in that they do not provide all the information to which law enforcement is authorized. Further, some of these partial capabilities cannot provide information in real-time.

It has been reported the government receives a daily dump of screen shots from companies. Why is this not good enough?

In some cases subject to legal process, it may be sufficient that law enforcement receives a daily report of a target's information. But in many instances, information provided in this manner is incomplete or not provided in a timely manner to support every type of investigative requirement, especially when dealing with reactive crimes (e.g., kidnapping, extortion, drug trafficking, terrorism). Also, not every company has this capability. Further, there is significant disparity in what companies offering similar services can provide to law enforcement – there is simply a lack of consistency across the board.

Does the FBI favor new electronic surveillance capability laws or see a need to update existing laws such as CALEA?

In certain respects, today's ever-widening gap between technology and law enforcement's electronic surveillance capabilities is not a new phenomenon. For decades, law enforcement has struggled to keep pace with evolving communications technology, periodically requiring congressional intervention to align law enforcement capabilities with new technological realities. The difference today is the sheer pace at which communications technology is advancing. Each passing year brings a dramatic increase in the volume of communications,

the sophistication and complexity of communications service offerings, the number of communications service providers, and the use of encryption.

The same technology fueling this rapid innovation, however, is simultaneously making lawful interception of modern communications services increasingly less feasible. Unless corrective action is taken, lawful intercept capabilities will continue to erode and potentially become obsolete. Law enforcement needs assistance and cooperation from companies to comply with lawful court orders and has to have a way to help these companies understand what it needs, why it needs it, and how they can assist. All of this can be accomplished while still protecting privacy rights and providing network security and innovation.

How will passage of the Domestic Retention and Investigatory Powers (DRIP) legislation in the United Kingdom, which requires companies to retain customer communications data, impact the Going Dark problem in the US?

It is premature to comment on how the UK legislation will impact United States law enforcement's ability to effect court orders. However, it does reflect the fact that the UK is facing a similarly daunting challenge in conducting electronic surveillance.

For any additional questions, including the FBI's use of show cause orders when companies refuse to comply with a court order, or the FBI's National Domestic Communications Assistance Center, please refer to headquarters.